WHAT IS CLAIMED IS:

Sub a1

1. A method for distributing computer software from a first computer system, comprising:

receiving a request for software from a second computer system;

generating a message;

encrypting the generated message;

transmitting the encrypted message to the second computer system;

receiving an encrypted response from the second computer system;

processing the encrypted response to determine whether the second computer system is authorized to access the software; and

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

2. The method of claim 1, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

3. The method of claim 1, further comprising transmitting the software to the second computer system after permitting access.

4. The method of claim 1, wherein generating the message further comprises generating a random component to include within the message.

5. The method of claim 1 wherein the random component is comprised of a time stamp.

6. The method of claim 4, wherein the time stamp is inserted at an offset into the message.

7. The method of claim 1, wherein the software comprises a computer program, further comprising automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

a1

8. The method of claim 1, wherein processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

9. The method of claim 8, wherein encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein processing the encrypted response further comprises decrypting the encrypted response with the public key of the second computer system.

10. The method of claim 1, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

11. The method of claim 10, wherein the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the first computer system maintains a public key associated with the second computer system that is the only key capable of decrypting the encrypted message.

a'

12. A method for accessing computer software from a first computer system with a second computer system, comprising:

transmitting a request for the software to the first computer system;

receiving an encrypted message from the first computer system;

processing the encrypted message to generate a response message;

transmitting the response message to the first computer system; and

receiving access to the requested software in response to the response message.

13. The method of claim 12, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

14. The method of claim 12, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

encrypting the decrypted message with the second computer system's private key; and

transmitting the message encrypted with the second computer system's private key to the first computer system.

15. The method of claim 12, wherein the received encrypted message includes a random component and a request for configuration data from the second computer system, further comprising adding configuration data for the second computer system to the decrypted message before encrypting the message with the second computer system's private key

16. A system for distributing computer software from a first computer system, comprising:

means for receiving a request for software from a second computer system;

means for generating a message;

means for encrypting the generated message;

means for transmitting the encrypted message to the second computer system;

means for receiving an encrypted response from the second computer system;

means for processing the encrypted response to determine whether the second computer system is authorized to access the software; and

means for permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

17. The system of claim 16, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

18. The system of claim 16, further comprising means for transmitting the software to the second computer system after permitting access.

19. The system of claim 16, wherein the means for generating the message further comprises generating a random component to include within the message.

a

20. The system of claim 16, wherein the software comprises a computer program, further comprising means for automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

21. The system of claim 16, wherein the means for processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

22. The system of claim 21, wherein the means for encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the means for processing the encrypted response further comprises decrypting the encrypted response with the public key of the second computer system.

23. The system of claim 16, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

24. The system of claim 23, wherein the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the first computer system maintains a public key associated with the second computer system that is the only key capable of decrypting the encrypted message.

25. A system for accessing computer software from a first computer system with a second computer system, comprising:

means for transmitting a request for the software to the first computer system;

means for receiving an encrypted message from the first computer system;

means for processing the encrypted message to generate a response message;

means for transmitting the response message to the first computer system; and

means for receiving access to the requested software in response to the response message.

26. The system of claim 25, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

means for decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

means for encrypting the decrypted message with the second computer system's private key; and

means for transmitting the message encrypted with the second computer system's private key to the first computer system.

27. An article of manufacture for use in distributing computer software from a first computer system the article of manufacture comprising computer usable media including at least one computer program embedded therein that causes the first computer system to perform:

receiving a request for software from a second computer system;

generating a message;

encrypting the generated message;

transmitting the encrypted message to the second computer system;

receiving an encrypted response from the second computer system;

processing the encrypted response to determine whether the second computer system is authorized to access the software; and

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

28. The article of manufacture of claim 27, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

29. The article of manufacture of claim 27, further comprising transmitting the software to the second computer system after permitting access.

30. The article of manufacture of claim 27, wherein generating the message further comprises generating a random component to include within the message.

31. The article of manufacture of claim 27, wherein the random component is comprised of a time stamp.

a

32. The article of manufacture of claim 30, wherein the time stamp is inserted at an offset into the message.

33. The article of manufacture of claim 27, wherein the software comprises a computer program, further comprising automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

34. The article of manufacture of claim 27, wherein processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

35. The article of manufacture of claim 34, wherein encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein

processing the encrypted response further comprises decrypting the encrypted response with the public key of the second computer system.

36. The article of manufacture of claim 37, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

37. The article of manufacture of claim 36, wherein the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the first computer system maintains a public key associated with the second computer system that is the only key capable of decrypting the encrypted message.

38. The article of manufacture of claim 27, the article of manufacture comprising at least one additional software program to cause the second computer system to perform:

transmitting a request for the software to the first computer system;

receiving an encrypted message from the first computer system;

processing the encrypted message to generate a response message;

transmitting the response message to the first computer system; and

receiving access to the requested software in response to the response message.

39. The article of manufacture of claim 38, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

encrypting the decrypted message with the second computer system's private key; and

transmitting the message encrypted with the second computer system's private key to the first computer system.

40. The article of manufacture of claim 38, wherein the received encrypted message includes a random component and a request for configuration data from the second computer system, further comprising adding configuration data for the second computer system to the decrypted message before encrypting the message with the second computer system's private key